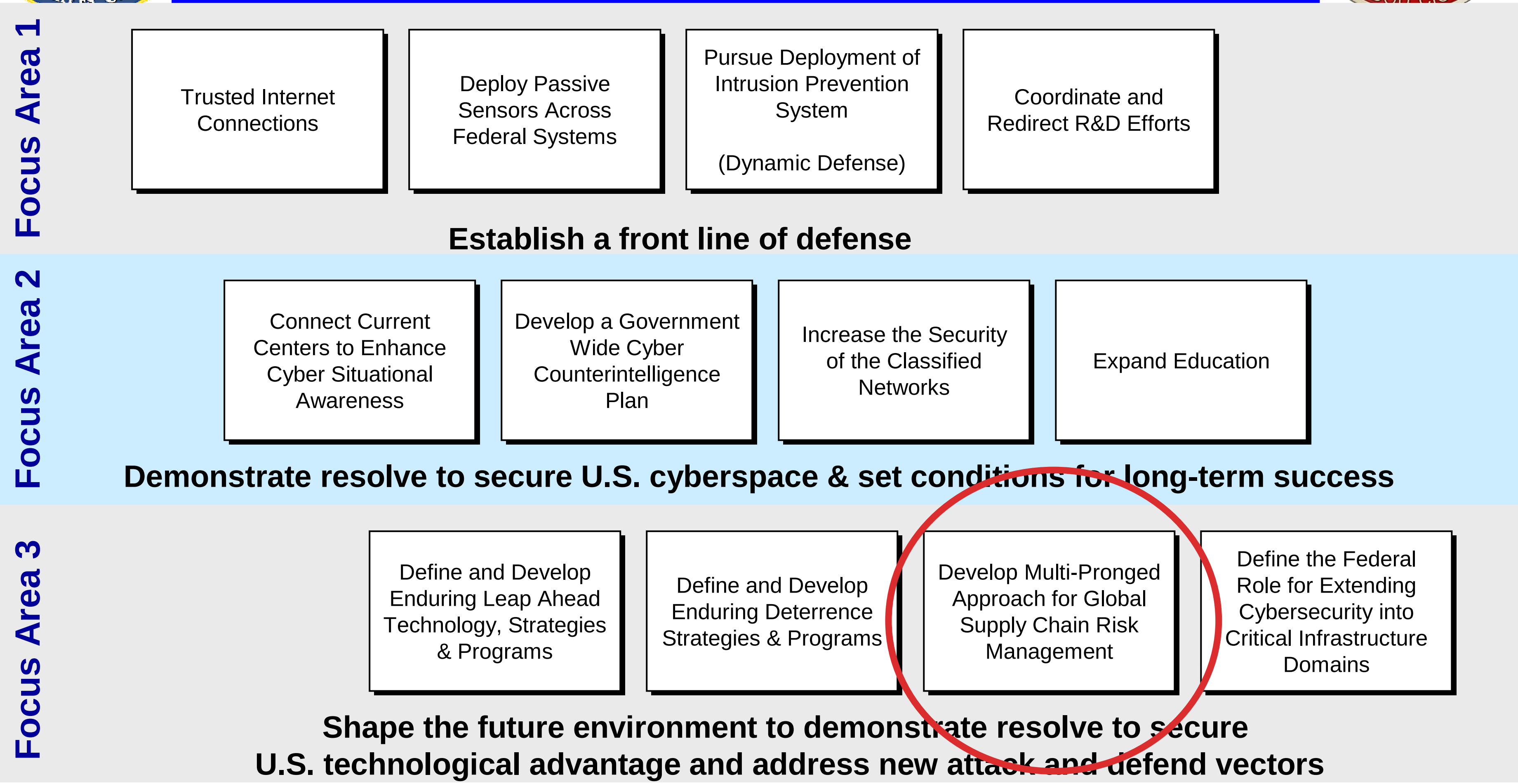
CNCI-SCRM

Don.Davidson@osd.mil
Globalization Task Force

Comprehensive National Cybersecurity Initiative (CNCI)



Focus Area 1

Trusted Internet Connections

Deploy Passive Sensors Across Federal Systems

Pursue Deployment of Intrusion Prevention System

(Dynamic Defense)

Coordinate and Redirect R&D Efforts

Establish a front line of defense

Focus Area 2

Connect Current Centers to Enhance Cyber Situational Awareness

Develop a Government Wide Cyber Counterintelligence Plan

Increase the Security of the Classified Networks

Expand Education

Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success

Focus Area 3

Define and Develop Enduring Leap Ahead Technology, Strategies & Programs

Define and Develop Enduring Deterrence Strategies & Programs

Develop Multi-Pronged Approach for Global Supply Chain Risk Management

Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains

Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

The Comprehensive National Cybersecurity Initiative also includes seven priority areas of foundational investment that are essential to enable these activities

SCRM Goal: Systems Assurance

Systems Assurance relates to the level of confidence that software, hardware, and systems function as intended in all circumstances, and are free of vulnerabilities, either intentionally or unintentionally designed or inserted throughout the lifecycle

1. Understand system criticality and prioritize to focus resources
2. Understand dependence on critical subcomponents and engineer systems for assurance
3. Understand supply chain for critical components and manage risk through acquisition
4. Utilize tools and techniques to detect and mitigate vulnerabilities
5. Partner with industry to drive security (manufacturing, engineering, test and evaluation, etc.)

Vision

Goal:
Systems Assurance

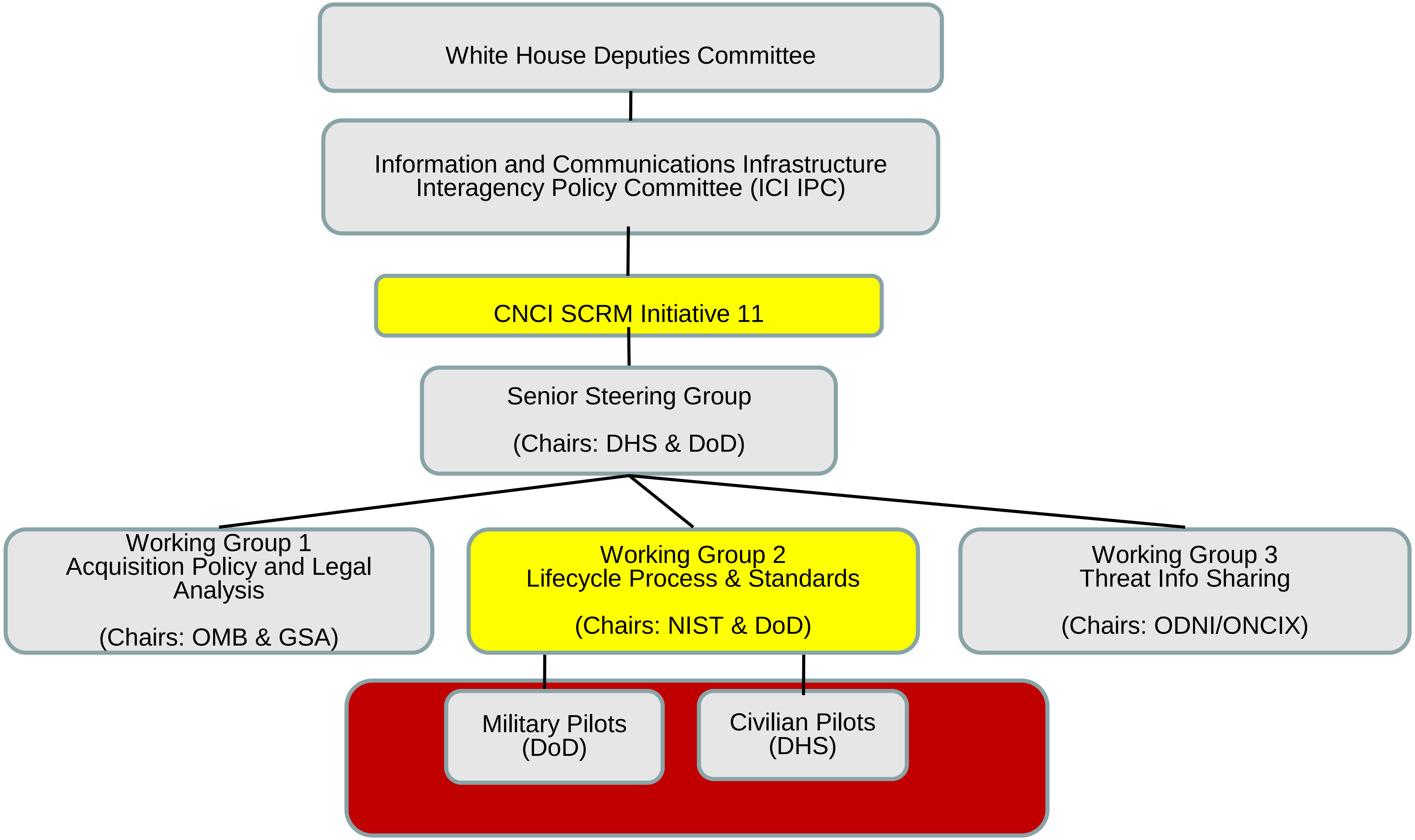
End State:
SCRM Capability

Program Managers will use SCRM resources in Program Protection Planning and Information Assurance processes to manage global ICT supply chain risk to mission critical systems and networks across DoD

SCRM Building Blocks

Policy ♦ Pilots ♦ Threat Assessment Center ♦ Centers of Excellence ♦ Technical Toolbox ♦ Legislative Proposal ♦ Commercial Global Sourcing Standards

CNCI Authorities



White House Deputies Committee

Information and Communications Infrastructure Interagency Policy Committee (ICI IPC)

CNCI SCRM Initiative 11

Senior Steering Group

(Chairs: DHS & DoD)

Working Group 1
Acquisition Policy and Legal Analysis

(Chairs: OMB & GSA)

Working Group 2
Lifecycle Process & Standards

(Chairs: NIST & DoD)

Working Group 3
Threat Info Sharing

(Chairs: ODNI/ONCIX)

Military Pilots
(DoD)

Civilian Pilots
(DHS)

Globalization Task Force (GTF)

- **Mission** – To develop and oversee implementation of a strategy for mitigating national security risks to DoD weapons systems and information networks arising from the globalization of ICT

- **Programs** –
  - *Supply Chain Risk Management (SCRM)*
    - Leads the development and implementation of DoD SCRM strategy
    - Co-leads interagency SCRM activities under the Comprehensive National Cybersecurity Initiative (CNCI), Initiative 11
  - *Transactional Risk Management (TRM)*
    - Leads DoD's analysis of direct foreign investment transactions involving ICT and U.S. telecommunications infrastructure
      - Committee on Foreign Investment in the United States (CFIUS)
      - Federal Communications Commissions transactions

Impact to DoD Programs and Processes

SCRM is a Multi-Disciplinary Solution Designed to Enable Assurance of Mission Critical Systems and Networks

SCRM:

- Strengthens operations security of acquisition processes in the face of supply chain attacks
- Drives awareness of supply chain vulnerabilities in systems engineering, making systems more robust
- Provides threat and risk assessments to program managers to:
  - Enhance the acquisition strategy before procurement
  - Technically mitigate risk after procurement
- Works with industry to:
  - Understand risk accepted by DoD via commercial ICT
  - Strengthen commercial supply chain practices

SCRM
Guiding Principles

- Defense-in-breadth: Mitigate risk across the entire lifecycle

- Understand risk management problem from a systems perspective
  - Response should be commensurate with risk and system/network criticality
  - Need to understand levels of vulnerability and threat relative to each system

- Develop higher assurance characteristics into commercial products where we have leverage

- Continued access to global ICT is critical to DoD mission

To meet tomorrow's threat we must develop protection measures across product lifecycle and reinforce these measures through USG acquisition processes and effective implementation of agency security practices

SCRM
Key Components

① **Supply Chain Information Sharing**

- DoD, Govt & Industry

② **Engineering**

- Develop acquisition and engineering guidance enabling SCRM
- Utilize global sourcing risk management standards and best practices from industry

③ **Procurement Tools**

- Supply chain -informed procurement remains challenge